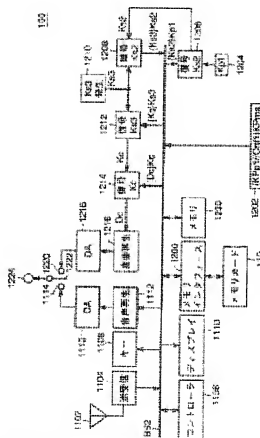


**Priority number(s):** JP20000287909 20000922

**SOLUTION:** A portable telephone set 100 includes a controller 1106, a display 1110, a key operation part 1108, a memory 1230, a memory card 110 and a reproduction system circuit. In a music reproducing mode, information (reproduced music list) on reproducible contents data is displayed on the display 1110 based on an inter-media music list recorded in the memory card 110. A user selects music from pertinent display. In a media managing mode, compiling work is possible corresponding to the inter-media music list showing the data contents recorded in the memory card 110.



<http://v3.espacenet.com/publicationDetails/biblio?adjacent=true&KC=A&date=20020405...> 3/20/2009

(51) Int.Cl. <sup>7</sup>	識別番号	F I	ターコード <sup>*</sup> (参考)
G 0 6 F 17/60	3 0 2	G 0 6 F 17/60	3 0 2 E 5 B 0 4 9
	1 3 2		1 3 2 5 J 1 0 4
	1 4 2		1 4 2
	5 0 6		5 0 6
G 0 9 C 1/00	6 6 0	G 0 9 C 1/00	6 6 0 D
審査請求 未請求 請求項の数13 O L (全 23 頁)			

(21) 出願番号 特願2000-287909 (P2000-287909)

(22) 出願日 平成12年9月22日 (2000.9.22)

(71) 出願人 000001889

三洋電機株式会社

大阪府守口市京阪本通2丁目5番5号

(72) 発明者 盛合 真介

大阪府守口市京阪本通2丁目5番5号 三

洋電機株式会社内

(74) 代理人 100064746

弁理士 深見 久郎 (外3名)

Fターム (参考) 5B049 AA02 AA05 CC09 DD01 EE05

FF07 GG03 GG04 GG07

5J104 AA01 AA16 EA04 EA15 NA02

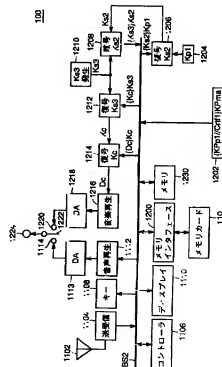
NA37 PA02 PA07 PA14

## (54) 【発明の名称】 データ再生装置およびライセンス管理方法

## (57) 【要約】

【課題】 選曲およびコンテンツの管理が簡便化した手続きで実現可能なデータ再生装置およびライセンス管理方法を提供する。

【解決手段】 携帯電話機100は、コントローラ1106、ディスプレイ1110、キー操作部1108、メモリ1230、メモ리카ード1110および再生系回路を含む。音楽再生モードでは、メモ리카ード1110に記録されるメディア内曲リストに基づき、再生可能なコンテンツデータの情報(再生曲リスト)をディスプレイ1110に表示する。ユーザは、当該表示から選曲する。メディア管理モードでは、メモ리카ード1110に記録されるデータ内容を示すメディア内曲リストに対し、編集作業を可能とする。



## 【特許請求の範囲】

【請求項1】 コンテンツデータを暗号化した暗号化コンテンツデータと、前記暗号化コンテンツデータに関するライセンス情報とをダウンロードしてデータ記録装置に記録し、前記データ記録装置に記録された前記暗号化コンテンツデータを再生するデータ再生装置であって、外部との通信を行う通信部と、データ授受を制御するインタフェースと、制御部と、表示部とを備え、前記制御部は、前記再生時に、再生可能な前記暗号化コンテンツデータに関するコンテンツリストを前記表示部に表示する、データ再生装置。

【請求項2】 前記コンテンツリストのなかから再生する前記暗号化コンテンツデータが選択される、請求項1に記載のデータ再生装置。

【請求項3】 前記制御部は、前記データ記録装置に記録されるデータに基づき、コンテンツ毎に、前記暗号化コンテンツデータおよび前記ライセンス情報、前記暗号化コンテンツデータのみ、または前記ライセンス情報のみが存在することを示す情報を含むメディア内コンテンツリストを生成し、前記再生時において、前記メディア内コンテンツリストに基づき、前記コンテンツリストを生成する、請求項1に記載のデータ再生装置。

【請求項4】 前記データ記録装置は、記録されるデータに基づき、コンテンツ毎に、前記暗号化コンテンツデータおよび前記ライセンス情報、前記暗号化コンテンツデータのみ、または前記ライセンス情報のみが存在することを示す情報を含むメディア内コンテンツリストを生成し、前記制御部は、前記再生時において、前記メディア内コンテンツリストに基づき、前記コンテンツリストを生成する、請求項1に記載のデータ再生装置。

【請求項5】 前記制御部は、前記データ記録装置に記録されるデータに基づき、コンテンツ毎に、前記ライセンス情報により再生に制限があるか否かを示す情報を含むメディア内コンテンツリストを生成し、前記再生時において、前記メディア内コンテンツリストに基づき、前記コンテンツリストを生成する、請求項1に記載のデータ再生装置。

【請求項6】 前記データ記録装置は、記録されるデータに基づき、コンテンツ毎に、前記ライセンス情報により再生に制限があるか否かを示す情報を含むメディア内コンテンツリストを生成し、前記制御部は、前記再生時において、前記メディア内コンテンツリストに基づき、前記コンテンツリストを生成する、請求項1

に記載のデータ再生装置

【請求項7】 前記制御部は、前記暗号化コンテンツデータおよび前記ライセンス情報の双方が存在するコンテンツに関する情報を表示する、請求項1に記載のデータ再生装置。

【請求項8】 前記制御部は、前記再生時において、前記ライセンス情報に基づき再生不可能になった前記暗号化コンテンツデータに関する情報については、前記コンテンツリストから削除する、請求項1から7のいずれか1項に記載のデータ再生装置。

【請求項9】 前記制御部は、メディア管理モードでは、前記メディア内コンテンツリストを前記表示部に表示し、

前記表示部に表示される前記メディア内コンテンツリストにおいて変更可能なデータを編集するための回路をさらに備える、請求項3、4、5、6のいずれか1項に記載のデータ再生装置

【請求項10】 コンテンツデータを暗号化した暗号化コンテンツデータと、前記暗号化コンテンツデータに関するライセンス情報とをダウンロードしてデータ記録装置に記録し、前記データ記録装置に記録された前記暗号化コンテンツデータを再生するデータ再生装置におけるライセンス管理方法であって、モードを判定するステップと、前記判定により再生モードであると判定される場合に、再生可能な前記暗号化コンテンツデータに関するコンテンツリストを生成するステップと、前記コンテンツリストを表示する表示ステップとを含む再生ステップと備える、ライセンス管理方法。

【請求項11】 前記再生ステップは、前記再生時において、前記ライセンス情報に基づき再生不可能になった前記暗号化コンテンツデータについては、前記コンテンツリストから削除するステップを含む、請求項10に記載のライセンス管理方法。

【請求項12】 前記データ記録装置に記録されるデータに基づき、メディア内コンテンツリストを生成するステップをさらに備え、前記コンテンツリストは、前記メディア内コンテンツリストに基づき生成される、請求項10に記載のライセンス管理方法。

【請求項13】 前記モードを判定するステップにおいてメディア管理モードであると判定される場合に、前記メディア内コンテンツリストにおいて変更可能なデータを編集することができるステップをさらに備える、請求項12に記載のライセンス管理方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 この発明は、コピーされた情報に対する著作権保護を可能とするデータ配信システムにおいて用いられるデータ再生装置およびライセンス管

理方法に関するものである。

【0002】

【従来の技術】近年、インターネット等の情報通信網等の進歩により、携帯電話機等を用いた個人向け端末により、各ユーザが容易にネットワーク情報にアクセスすることが可能となっている。

【0003】このような情報通信網においては、デジタル信号により情報が伝送される。したがって、たとえば上述のような情報通信網において伝送された音楽や映像データ等各個人ユーザがコピーした場合でも、そのようなコピーによる音質や画質の劣化をほとんど生じさせることなく、データのコピーを行なうことが可能である。

【0004】したがって、このような情報通信網上において音楽データや画像データ等の著作権者の権利が存在する創作物が伝送される場合、適切な著作権保護のための方策が取られていないと、著しく著作権者の権利が侵害されてしまうおそれがある。

【0005】音楽データや画像データをデジタル情報通信網を通じて公衆に配信することは、それ自体が著作権者の公衆送信権による制限を受ける行為であるから、著作権保護のための十分な方策が講じられる必要がある。

【0006】

【発明が解決しようとする課題】ところで、コンテンツデータを再生するための復号鍵（ライセンス）には、再生回数制限や期日制限などを設定することができる。

【0007】しかし、著作権保護が必要とされるコンテンツデータを復号する（再生する）場合に、ユーザがその都度ライセンス状態を確認する必要があるとすれば、ユーザ側にとって再生手続きが煩雑になる。

【0008】また、ユーザ側は、このようなダウンロードしたコンテンツデータを簡単な手続きで管理したいという要望もある。

【0009】そこで、本発明は、かかる問題を解決するためになされたものであり、その目的は、再生モードにおいて、自動的にライセンス状態を判別して再生可能な暗号化コンテンツデータを提示することができるデータ再生装置およびライセンス管理方法を提供することである。

【0010】また、さらなる目的は、ダウンロードした暗号化コンテンツデータを簡単な手続きで管理することができるデータ再生装置およびライセンス管理方法を提供することである。

【0011】

【課題を解決するための手段および発明の効果】この発明のある局面によるデータ再生装置は、コンテンツデータを暗号化した暗号化コンテンツデータと、暗号化コンテンツデータに関するライセンス情報とをダウンロードしてデータ記録装置に記録し、データ記録装置に記録された暗号化コンテンツデータを再生するデータ再生装置であって、外部との通信を行なう通信部と、データ授受

を制御するインタフェースと、制御部と、表示部とを備える。制御部は、再生時に、再生可能な暗号化コンテンツデータに関するコンテンツリストを表示部に表示する。

【0012】好ましくは、コンテンツリストのなかから再生される暗号化コンテンツデータが選択される。

【0013】好ましくは、制御部は、データ記録装置に記録されるデータに基づき、メディア内コンテンツリストを生成し、再生時において、メディア内コンテンツリストに基づき、コンテンツリストを生成する。

【0014】好ましくは、データ記録装置は、記録されるデータに関する情報を含むメディア内コンテンツリストを生成し、制御部は、再生時において、メディア内コンテンツリストに基づき、コンテンツリストを生成する。

【0015】メディア内コンテンツリストは、コンテンツ毎に、暗号化コンテンツデータおよびライセンス情報、暗号化コンテンツデータのみ、またはライセンス情報のみが存在することを明示する情報を含む。また、メディア内コンテンツリストは、コンテンツ毎に、ライセンス情報により再生に制限があるか否かを示す情報を含む。

【0016】特に、制御部は、暗号化コンテンツデータおよびライセンス情報の双方が存在するコンテンツに関する情報を表示する。

【0017】特に、制御部は、再生時において、ライセンス情報に基づき再生不可能になった暗号化コンテンツデータについては、コンテンツリストから削除する。

【0018】特に、制御部は、メディア管理モードでは、メディア内コンテンツリストを表示部に表示し、表示部に表示されるメディア内コンテンツリストにおいて変更可能なデータを編集するための回路をさらに備える。

【0019】この発明のさらなる局面によるライセンス管理方法は、コンテンツデータを暗号化した暗号化コンテンツデータと、暗号化コンテンツデータに関するライセンス情報とをダウンロードしてデータ記録装置に記録し、データ記録装置に記録された暗号化コンテンツデータを再生するデータ再生装置におけるライセンス管理方法であって、モードを判定するステップと、判定により再生モードであると判定される場合に、再生可能な暗号化コンテンツデータに関するコンテンツリストを生成するステップと、コンテンツリストを表示する表示ステップとを含む再生ステップと備える。

【0020】好ましくは、再生ステップは、再生時に、ライセンス情報に基づき再生不可能になった暗号化コンテンツデータについては、コンテンツリストから削除するステップをさらに含む。

【0021】好ましくは、データ記録装置に記録されるデータに基づき、メディア内コンテンツリストを生成す

るステップをさらに備え、コンテンツリストは、メディア内コンテンツリストに基づき生成される。

【0022】特に、モードを判定するステップにおいて、メディア管理モードであると判定される場合に、メディア内コンテンツリストにおいて変更可能なデータを編集することができるとするステップに備える。

【0023】したがって、この発明によれば、再生側において、ライセンスの制限を自動的に判別できるため、ユーザ側の選曲動作が簡単化される。また、コンテンツに関する変更可能なデータをユーザ側で編集することができると、ユーザ側の意向にそったデータ管理が可能になる。

【0024】

【発明の実施の形態】本発明の実施の形態について図面を参照しながら詳細に説明する。なお、図中同一または相当部分には同一符号を付してその説明は繰返さない。

【0025】[第1の実施の形態] 図1は、本発明によるデータ端末装置が再生の対象とする暗号化コンテンツデータをメモリカードへ配信するデータ配信システムの全体構成を概念的に説明するための概略図である。

【0026】なお、以下では携帯電話機を介してデジタル音楽データを各携帯電話ユーザに配信するデータ配信システム構成を例にとって説明するが、以下の説明で明らかとなるように、本発明はこのような場合に限定されることなく、他の著作物としてのコンテンツデータ、たとえば画像データ、動画係データ等を配信する場合においても適用することが可能なものである。また、他の情報通信網を介して配信する場合においても適用可能である。

【0027】図1を参照して、著作権の存在する音楽データを管理するライセンスサーバ10は、データ配信を求めてアクセスして来た携帯電話ユーザ1の携帯電話機100に装着されたメモリカード110が正当な認証データを持つか否か、すなわち、正規のメモリカードであるか否かの認証処理を行ない、正当なメモリカードに対して所定の暗号方式により音楽データ（以下コンテンツデータとも呼ぶ）を暗号化した上で、データを配信するための配信キャリア20である携帯電話会社に、このような暗号化コンテンツデータを与える。

【0028】配信キャリア20は、自己の携帯電話網を通じて、各携帯電話ユーザからの配信要求（配信リクエスト）をライセンスサーバ10に中継する。ライセンスサーバ10は、配信リクエストがあると、メモリカード等が正規の機器であることを確認し、要求されたコンテンツデータをさらに暗号化した上で配信キャリア20の携帯電話網を介して、各携帯電話ユーザの携帯電話機を介して装着されたメモリカードに対してコンテンツデータを配信する。

【0029】図1においては、たとえば携帯電話ユーザ1の携帯電話機100には、着脱可能なメモリカード1

10が装着される構成となっている。メモリカード110は、携帯電話機100により受信された暗号化コンテンツデータを受取り、格納する。また、上記配信にあたって行なわれた認証処理によりライセンスキーを受取り、データを格納する。暗号化を復号した上で、携帯電話機100中の音楽再生部（図示せず）に与える。

【0030】さらに、たとえば携帯電話ユーザは、携帯電話機100に接続したヘッドホン130等を介してライセンスキーにより暗号化コンテンツデータを復号して「再生」し、聴取することが可能である。

【0031】以下では、このようなライセンスサーバ10と配信キャリア20と併せて、配信サーバ30と総称することとする。

【0032】また、このような配信サーバ30から、各携帯電話機等にコンテンツデータを伝送する処理を「配信」と称することとする。

【0033】このような構成とすることで、まず、メモリカード110を利用しないと、配信サーバ30からコンテンツデータの配信を受けて、音楽を再生することが困難な構成となる。

【0034】しかも、配信キャリア20において、たとえば1曲分のコンテンツデータを配信するたびにその度数を数計しておくことで、携帯電話ユーザがコンテンツデータを受信（ダウンロード）するたびに発生する著作権料を、配信キャリア20が携帯電話機の通話料とともに徴収することとすれば、著作権者が著作権料を確保することが容易となる。

【0035】このような構成において、暗号化して配信されるコンテンツデータを携帯電話のユーザ側で再生可能とするためにシステム上必要とされるのは、第1には、通信における暗号化鍵を配信するための方式である。第2には、配信したいコンテンツデータを暗号化する方式そのものである。第3には、このように配信されたコンテンツデータの無断コピーを防止するためのコンテンツデータ保護を実現する構成である。

【0036】そして、第4には、再生モードにおいて、ライセンス状態を自動的に判別するための構成である。さらに、第5には、コンテンツに関するリストをユーザが編集可能とするための構成である。

【0037】第1の実施の形態においては、特に、配信、および再生の各セッションの発生時において、これらのコンテンツデータの移動先に対する認証およびチェック機能を充実させ、非認証もしくは復号鍵の破られた記録装置およびコンテンツ再生装置（携帯電話機）に対するコンテンツデータの出力を防止することによってコンテンツデータの著作権保護を強化する構成、ならびにコンテンツデータに関するリストをユーザに提示するとともに、ユーザ側で当該リストの編集を行える構成を示す。

【0038】図2は、図1に示したデータ配信システム

において、使用される通信のためのデータ、情報等の特性を説明する図である。

【0039】まず、配信サーバ30より配信されるデータについて説明する。Dataは、音楽データ等のコンテンツデータである。コンテンツデータDataには、ライセンスキーKcで復号可能な暗号化が施される。ライセンスキー（「コンテンツ鍵」とも言う。以下同じ。）Kcによって復号可能な暗号化が施された暗号化コンテンツデータ{Data}Kcがこの形式で配信サーバ30より携帯電話ユーザに配布される。

【0040】なお、以下においては、{Y}Xという表記は、データYを、復号鍵Xにより復号可能な暗号化を施したことを示すものとする。

【0041】さらに、配信サーバ30からは、暗号化コンテンツデータとともに、コンテンツデータに関する著作権あるいはサーバアクセス関連等の平文情報としての付加情報Data-infが配布される。また、ライセンス情報としては、コンテンツデータDataを識別するためのコードであるコンテンツIDおよびライセンスの発行を特定できる管理コードであるライセンスIDや、利用者側からの指定によって決定されるライセンス数や機能限定等の情報を含んだライセンス購入条件ACに基づいて生成される、メモリのアクセスに対する制限に関する情報であるアクセス制限情報AC1および再生回路における制御情報である再生回路制御情報AC2が存在する。以後、ライセンスキーKcとコンテンツIDとライセンスIDとアクセス制限情報AC1と再生回路制御情報AC2とを併せて、ライセンスと総称することとする。

【0042】図3は、図1に示すデータ配信システムにおいて使用される認証および禁止クラスリストの運用のためのデータ、情報等の特性を説明する図である。

【0043】第1の実施の形態においては、記録装置（メモリカード）やコンテンツデータを再生するデータ端末装置（携帯電話機）のクラスとして、コンテンツデータの配信、および再生を禁止することができるように禁止クラスリストCRL（Class Revocation List）の運用を行なう。以下では、必要に応じて記号CRLによって禁止クラスリスト内のデータを表わすこともある。

【0044】禁止クラスリスト関連情報には、ライセンスの配信、および再生が禁止されるデータ端末装置およびメモリカードのクラスをリストアップした禁止クラスリストデータCRLが含まれる。

【0045】禁止クラスリストデータCRLは、配信サーバ30内で管理されるとともに、メモリカード内にも記録保持される。このような禁止クラスリストは、随時バージョンアップしデータを更新していく必要があるが、データの変更については、基本的には変更点のみを反映した差分データCRL\_datを配信サーバ30側

より発生して、これに応じてメモリカード内の禁止クラスリストCRLが書き換えられる構成とする。また、禁止クラスリストのバージョンについては、CRL\_verをメモリカード側より出力し、これを配信サーバ30側で確認することによってバージョン管理を実行する。差分データCRL\_datには新たなバージョンの情報も含まれる。また、バージョン情報として、更新日時を用いることも可能である。

【0046】このように、禁止クラスリストCRLを、配信サーバのみならずメモリカード内においても保持運用することによって、クラス固有すなわち、データ端末装置およびメモリカードの種類に固有の復号鍵が破られた、データ端末装置およびメモリカードへのライセンスキーの供給を禁止する。このため、データ端末装置ではコンテンツデータの再生が、メモリカードではコンテンツデータの移動が行えなくなる。

【0047】このように、メモリカード内の禁止クラスリストCRLは配信時に逐次データを更新する構成とする。また、メモリカード内における禁止クラスリストCRLの管理は、上位レベルとは独立にメモリカード内でタンパレジスタンスモジュール（Tamper Resistance Module）に記録する等によって、ファイルシステムやアプリケーションプログラム等によって上位レベルから禁止クラスリストデータCRLを改ざんすることが不可能な構成とする。この結果、データに関する著作権保護をより強固なものとすることができる。

【0048】データ端末装置およびメモリカードには固有の公開暗号鍵KpnnおよびKpmciがそれぞれ設けられ、公開暗号鍵KpnnおよびKpmciはデータ端末装置に固有の秘密復号鍵Kpnnおよびメモリカード固有の秘密復号鍵Kmcicによってそれぞれ復号可能である。これら公開暗号鍵および秘密復号鍵は、データ端末装置の種類ごとおよびメモリカードの種類ごとに異なる値を持つ。これらの公開暗号鍵および秘密復号鍵を総称してクラス鍵と称する。

【0049】また、再生回路およびメモリカードのクラス証明書として、CrtfnおよびCmcicがそれぞれ設けられる。

【0050】これらのクラス証明書は、メモリカードおよびコンテンツ再生部（携帯電話機）のクラスごとに異なる情報を有する。クラス鍵による暗号が破られた、すなわち、秘密復号鍵が取得されたクラス鍵に対しては、禁止クラスリストにリストアップされてライセンス発行の禁止対象となる。

【0051】これらのメモリカードおよびコンテンツ再生部固有の公開暗号鍵およびクラス証明書は、認証データ{Kpmci//Cmcic}Kpmaおよび{Kpnn//Crtfn}Kpmaの形式で、出荷時にメモリカードおよび携帯電話機にそれぞれ記録される。後ほど

詳細に説明するが、K P m aは配信システム全体で共通の公開認証鍵である。

【0052】図4は、図1に示したデータ配信システムにおいて暗号化に関わる鍵の特性をまとめて説明する図である。

【0053】メモ리카ード外とメモ리카ード間でのデータ授受における秘密保持のための暗号鍵として、コンテンツデータの配信、および再生が行なわれるごとに配信サーバ30、携帯電話機100、メモ리카ード110において生成される共通鍵K s 1〜K s 3が用いられる。

【0054】ここで、共通鍵K s 1〜K s 3は、配信サーバ、携帯電話機もしくはメモ리카ード間の通信の単位あるいはアクセスの単位である「セッション」ごとに発生する固有の共通鍵であり、以下においてはこれらの共通鍵K s 1〜K s 3を「セッションキー」とも呼ぶこととする。

【0055】これらのセッションキーK s 1〜K s 3は、各通信セッションごとに固有の値を有することにより、配信サーバ、携帯電話機およびメモ리카ードによって管理される。具体的には、セッションキーK s 1は、配信サーバによって配信セッションごとに発生される。セッションキーK s 2は、メモ리카ードによって配信セッションおよび再生セッションごとに発生し、セッションキーK s 3は、携帯電話機において再生セッションごとに発生される。各セッションにおいて、これらのセッションキーを授受し、他の機器で生成されたセッションキーを受けて、このセッションキーによる暗号化を実行したうえでライセンスキー等の送信を行なうことによって、セッションにおけるセキュリティ強度を向上させることができる。

【0056】また、メモ리카ード110内のデータ処理を管理するための鍵として、メモ리카ードという媒体ごとに設定される公開暗号鍵K p mと、公開暗号鍵K p mで暗号化されたデータを復号することが可能なメモ리카ードごとに固有の秘密復号鍵K mが存在する。

【0057】図5は、図1に示したライセンスサーバ100の構成を示す概略ブロック図である。

【0058】ライセンスサーバ100は、コンテンツデータを所定の方式に従って暗号化したデータや、ライセンスID等の配信情報を保持するための情報データベース304と、各携帯電話ユーザごとにコンテンツデータへのアクセス開始に従った課金情報を保持するための課金データベース302と、禁止クラスリストCRLを管理するCRLデータベース306と、情報データベース304、課金データベース302およびCRLデータベース306からのデータをデータバスBS1を介して受取り、所定の処理を行なうためのデータ処理部310と、通信網を介して、配信キャリア20とデータ処理部310との間でデータ授受を行なうための通信装置350とを備える。

【0059】データ処理部310は、データバスBS1上のデータに応じて、データ処理部310の動作を制御するための配信制御部315と、配信制御部315に制御されて、配信セッション時にセッションキーK s 1を発生するためのセッションキー発生部316と、メモ리카ードおよび携帯電話機から送られてきた認証のための認証データ {K P m c i // C m c i} K P m aを通信装置350およびデータバスBS1を介して受けて、公開認証鍵K P m aによる復号処理を行なう復号処理部312と、セッションキー発生部316より生成されたセッションキーK s 1を復号処理部312によって得られた公開暗号鍵K P m c iを用いて暗号化して、データバスBS1に出力するための暗号化処理部318と、セッションキーK s 1によって暗号化された上で送信されたデータをデータバスBS1より受けて、復号処理を行なう復号処理部320を含む。

【0060】データ処理部310は、さらに、配信制御部315から与えられるライセンスキーK cおよび再生回路制御情報AC2を、復号処理部320によって得られたメモ리카ード固有の公開暗号鍵K p mによって暗号化するための暗号化処理部326と、暗号化処理部326の出力を、復号処理部320から与えられるセッションキーK s 2によってさらに暗号化してデータバスBS1に出力するための暗号化処理部328を含む。

【0061】ライセンスサーバ100の配信セッションにおける動作については、後ほどフローチャートを使用して詳細に説明する。

【0062】図6は、図1に示した携帯電話機100の構成を説明するための概略ブロック図である。

【0063】携帯電話機100は、携帯電話網により無線伝送される信号を受信するためのアンテナ1102と、アンテナ1102からの信号を受けてベースバンド信号に変換し、あるいは携帯電話機からのデータを変換してアンテナ1102に与えるための送受信部1104と、携帯電話機100の各部のデータ授受を行なうためのデータバスBS2と、データバスBS2を介して携帯電話機100の動作を制御するためのコントローラ1106を含む。

【0064】携帯電話機100は、さらに、外部からの指示を携帯電話機100に与えるためのキー操作部1108と、コントローラ1106等から出力される情報を携帯電話ユーザに視覚情報として与えるためのディスプレイ1110と、通常の通話動作において、データバスBS2を介して与えられる受信データに基づいて音声再生するための音声再生部1112を含む。

【0065】携帯電話機100は、さらに、音声再生部1112の出力をデジタル信号からアナログ信号に変換するDA変換器1113と、DA変換器1113の出力を外部出力装置等へ出力するための端子1114とを含む。

【0066】携帯電話機100は、さらに、配信サーバ30からのコンテンツデータ（音楽データ）を記憶しかつ復号化処理するための着脱可能なメモリカード110と、メモリカード110とデータバスBS2との間のデータの授受を制御するためのメモリインタフェース1200を含む。

【0067】携帯電話機100は、さらに、携帯電話機の種類（クラス）ごとにそれぞれ設定される、公開暗号鍵Kp1およびクラス証明書Crtf1を公開復号鍵Kpmaで復号することでその正当性を認証できる状態に暗号化した認証データ{Kp1//Crtf1}Kpmaを保持する認証データ保持部1202を含む。

【0068】携帯電話機100は、さらに、携帯電話機（コンテンツ再生回路）固有の復号鍵であるKp1を保持するKp1保持部1204と、データバスBS2から受けたデータをKp1によって復号しメモリカード110によって発生されたセッションキーKs2を得る復号処理部1206を含む。

【0069】携帯電話機100は、さらに、メモリカード110に記憶されたコンテンツデータの再生を行なう再生セッションにおいてメモリカード110との間でデータバスBS2上においてやり取りされるデータを暗号化するためのセッションキーKs3を乱数等により発生するセッションキー発生部1210と、生成されたセッションキーKs3を復号処理部1206によって得られたセッションキーKs2によって暗号化しデータバスBS2に出力する暗号化処理部1208を含む。

【0070】携帯電話機100は、さらに、データバスBS2上のデータをセッションキーKs3によって復号して出力する復号処理部1212を含む。

【0071】携帯電話機100は、さらに、データバスBS2より暗号化コンテンツデータ{Data}Kcを受けて、復号処理部1212より取得したライセンスキーKcによって復号しコンテンツデータを出力する復号処理部1214と、復号処理部1214の出力を受けてコンテンツデータを再生するための音楽再生部1216と、音楽再生部1216の出力をデジタル信号からアナログ信号に変換するDA変換器1218と、DA変換器1218とDA変換器1218との出力を受けて、動作モードに応じて選択的に端子114または端子1220から出力するためのスイッチ1222と、スイッチ1222の出力を受けて、ヘッドホン130と接続するための接続端子1224と、データを記録するメモリ1230を含む。

【0072】コントローラ1106は、データダウンロード処理、データの再生処理、電源制御処理等を行うとともに、再生曲リストの生成、メディア管理モードでのメディア曲リストの生成、表示制御等を行う。

【0073】なお、図6においては、説明の簡素化のため、携帯電話機のうち本発明の音楽データの配信および

再生にかかわるブロックのみを記載し、携帯電話機が本来備えている通話機能に関するブロックについては、一部記載を省略している。

【0074】携帯電話機100の各構成部分の各セッションにおける動作については、後ほどフローチャートを使用して詳細に説明する。

【0075】図7は、メモリカード110の構成を説明するための概略ブロック図である。既に説明したように、メモリカードに固有の公開暗号鍵および秘密復号鍵として、Kpmc1およびKmc1が設けられ、メモリカードのクラス証明書Cmc1が設けられるが、メモリカード110においては、これらは自然数*i*=1でそれぞれ表わされるものとする。

【0076】したがって、メモリカード110は、認証データ{Kpmc1//Cmc1}Kpmaを保持する認証データ保持部1400と、メモリカードの種類ごとに設定される固有の復号鍵であるKmc1を保持するKmc1保持部1402と、メモリカードごとに固有に設定される秘密復号鍵Km1を保持するKm1保持部1421と、Km1によって復号可能な公開暗号鍵Kpmlを保持するKpml保持部1416を含む。認証データ保持部1400は、メモリカードの種類およびクラスごとにそれぞれ設定される公開暗号鍵Kpmc1およびクラス証明書Cmc1を公開認証鍵Kpmaで復号することでその正当性を認証できる状態に暗号化した認証データ{Kpmc1//Cmc1}Kpmaとして保持する。

【0077】このように、メモリカードという記録装置の暗号鍵を設けることによって、以下の説明で明らかになるように、配信されたコンテンツデータや暗号化されたライセンスキーの管理をメモリカード単位で実行することが可能になる。

【0078】メモリカード110は、さらに、メモリインタフェース1200との間で信号を端子1201を介して授受するデータバスBS3と、データバスBS3にメモリインタフェース1200から与えられるデータから、メモリカードの種類ごとに固有の秘密復号鍵Kmc1をKmc1保持部1402から受けて、配信サーバ30が配信セッションにおいて生成したセッションキーKs1を接点Paに出力する復号処理部1404と、Kpma保持部1414から認証鍵Kpmaを受けて、データバスBS3に与えられるデータからKpmaによる復号処理を実行して復号結果を暗号化処理部1410に出力する復号処理部1408と、切換スイッチ1442によって選択的に与えられる鍵によって、切換スイッチ1444によって選択的に与えられるデータを暗号化してデータバスBS3に出力する暗号化処理部1406を含む。

【0079】メモリカード110は、さらに、配信、および再生の各セッションにおいてセッションキーKs2



を発生するセッションキー発生部1418と、セッションキー発生部1418の出力したセッションキーKs2を復号処理部1408によって得られる公開暗号鍵K<sub>Pm</sub>もしくはK<sub>Pmc</sub>によって暗号化してデータバスBS3に送出する暗号化処理部1410と、データバスBS3よりセッションキーKs2によって暗号化されたデータを受けてセッションキー発生部1418より得たセッションキーKs2によって復号し、復号結果をデータバスBS4に送出する復号処理部1412を含む。

【0080】メモ리카ード110は、さらに、データバスBS3上のデータを公開暗号鍵K<sub>Pm</sub>1と対をなすメモ리카ード110固有の秘密復号鍵K<sub>m</sub>1によって復号するための復号処理部1422と、公開暗号鍵K<sub>Pm</sub>1で暗号化されている、ライセンスキーKc、再生回路制御情報AC2および再生情報(コンテンツID、ライセンスID、アクセス制御情報AC1)と、暗号化されていない禁止クラスリストのバージョン更新のための差分データCRL<sub>dat</sub>によって逐次更新される禁止クラスリストデータCRLとをデータバスBS4より受け取って格納するとともに、暗号化コンテンツデータ(Data)Kcおよび付加情報Data<sub>inf</sub>をバスBS3より受け取って格納するためのメモリ1415を含む。メモリ1415は、例えば半導体メモリによって構成される。

【0081】メモ리카ード110は、さらに、復号処理部1422によって得られるライセンスID、コンテンツIDおよびアクセス制限情報AC1を保持するためのライセンス情報保持部1440と、データバスBS3を介して外部との間でデータ授受を行い、データバスBS4との間で再生情報等を受けて、メモ리카ード110の動作を制御するためのコントローラ1420を含む。

【0082】ライセンス情報保持部1440は、データバスBS4との間でライセンスID、コンテンツIDおよびアクセス制限情報AC1のデータの授受が可能である。ライセンス情報保持部1440は、N個(N:自然数)のバンクを有し、各ライセンスに対応するライセンス情報をバンクごとに保持する。

【0083】なお、図7において、実線で囲んだ領域は、メモ리카ード110内において、外部からの不当な開封処理等が行なわれたと、内部データの消去や内部回路の破壊により、第三者に対してその領域内に存在する回路内のデータ等の読出を不能化するためのモジュールTRMに組込まれているものとする。このようなモジュールは、一般にはタンパーレジスタンスモジュール(Tamper Resistance Module)である。

【0084】もちろん、メモリ1415も含めて、モジュールTRM内に組込まれる構成としてもよい。しかしながら、図7に示したような構成とすることで、メモリ

1415中に保持されている再生に必要な再生情報は、いずれも暗号化されているデータであるため、第三者はこのメモリ1415中のデータのみでは、音楽を再生することは不可能であり、かつ高価なタンパーレジスタンスモジュール内にメモリ1415を設ける必要がないので、製造コストが低減されるという利点がある。

【0085】次に、図1に示すデータ配信システムの各セッションにおける動作についてフローチャートを参照して詳しく説明する。

【0086】図8および図9は、図1に示すデータ配信システムにおけるコンテンツの購入時に発生する配信動作(以下、配信セッションともいう)を説明するための第1および第2のフローチャートである。

【0087】図8および図9においては、携帯電話ユーザー1が、メモ리카ード110を用いることで、携帯電話機100を介して配信サーバ30から音楽データであるコンテンツデータの配信を受ける場合の動作を説明している。

【0088】まず、携帯電話ユーザー1の携帯電話機100から、携帯電話ユーザー1によるキー操作部1108のキーボタンの操作等によって、配信リクエストがなされる(ステップS100)。

【0089】メモ리카ード110においては、この配信リクエストに応じて、認証データ保持部1400より認証データ{K<sub>Pm</sub>1//Cmc1}K<sub>Pma</sub>が出力される(ステップS102)。

【0090】携帯電話機100は、メモ리카ード110からの認証のための認証データ{K<sub>Pm</sub>1//Cmc1}K<sub>Pma</sub>に加えて、コンテンツID、ライセンス購入条件のデータACとを配信サーバ30に対して送信する(ステップS104)。

【0091】配信サーバ30では、携帯電話機100からコンテンツID、認証データ{K<sub>Pm</sub>1//Cmc1}K<sub>Pma</sub>、ライセンス購入条件データACを受信し(ステップS106)、復号処理部312においてメモ리카ード110から出力された認証データを公開認証鍵K<sub>Pma</sub>で復号処理を実行する(ステップS108)。

【0092】配信制御部315は、復号処理部312における復号処理結果から、処理が正常に行なわれたか否か、すなわち、メモ리카ード110が正規のメモ리카ードからの公開暗号鍵K<sub>Pm</sub>1と証明書Cmc1を保持することを認証するために、正規の機関でその正当性を証明するための暗号を施した認証データを受信したか否かを判断する認証処理を行なう(ステップS110)。

正当な認証データであると判断された場合、配信制御部315は、公開暗号鍵K<sub>Pm</sub>1および証明書Cmc1を承認し、受理する。そして、次の処理(ステップS112)へ移行する。正当な認証データでない場合には、非承認とし、公開暗号鍵K<sub>Pm</sub>1および証明書Cmc1を受理しないで処理を終了する(ステップS17

0)。

【0093】認証の結果、正規の機器であることが認識されると、配信制御部315は、次に、メモ리카ード110のクラス証明書Cmc1が禁止クラスリストCRLにリストアップされているかどうかをCRLデータベース306に照会し、これらのクラス証明書が禁止クラスリストの対象になっている場合には、ここで配信セッションを終了する(ステップS170)。

【0094】一方、メモ리카ード110のクラス証明書が禁止クラスリストの対象外である場合には次の処理に移行する(ステップS112)。

【0095】認証の結果、正当な認証データを持つメモ리카ードを備える携帯電話機からのアクセスであり、クラスが禁止クラスリストの対象外であることが確認されると、配信サーバ30において、セッションキー発生部316は、配信のためのセッションキーKs1を生成する。セッションキーKs1は、復号処理部312によって得られたメモ리카ード110に対応する公開暗号鍵Kpmc1によって、暗号化処理部318によって暗号化される(ステップS114)。

【0096】暗号化されたセッションキーKs1は、{Ks1}Kmc1として、データバスBS1および通信装置350を介して外部に出力される(ステップS116)。

【0097】携帯電話機100が、暗号化されたセッションキー{Ks1}Kmc1を受信すると(ステップS118)、メモ리카ード110においては、メモリアインタフェース1200を介して、データバスBS3に与えられた受信データを、復号処理部1404が、保持部1402に保持されるメモ리카ード110固有の秘密復号鍵Kmc1により復号処理することにより、セッションキーKs1を復号し抽出する(ステップS120)。

【0098】コントローラ1420は、配信サーバ30で生成されたセッションキーKs1の受理を確認すると、セッションキー発生部1418に対して、メモ리카ード110において配信動作時に生成されるセッションキーKs2の生成を指示する。

【0099】また、配信セッションにおいては、コントローラ1420は、メモ리카ード110内のメモリ1415に記録されている禁止クラスリストの状態(バージョン)に関連する情報として、リストのバージョンデータCRL\_verをメモリ1415から抽出してデータバスBS4に出力する。

【0100】暗号化処理部1406は、切替スイッチ1442の接点Paを介して復号処理部1404より与えられるセッションキーKs1によって、切替スイッチ1444および1446の接点を順次切替えることによって与えられるセッションキーKs2、公開暗号鍵Kpmlおよび禁止クラスリストのバージョンデータCRL\_verを1つのデータ列として暗号化して、{Ks2/

/Kpml//CRL\_ver}Ks1をデータバスBS3に出力する(ステップS122)。

【0101】データバスBS3に出力された暗号化データ{Ks2//Kpml//CRL\_ver}Ks1は、データバスBS3から端子1201およびメモリアインタフェース1200を介して携帯電話機100に出力され、携帯電話機100から配信サーバ30に送信される(ステップS124)。

【0102】配信サーバ30は、暗号化データ{Ks2//Kpml//CRL\_ver}Ks1を受信して、復号処理部320においてセッションキーKs1による復号処理を実行し、メモ리카ード110で生成されたセッションキーKs2、メモ리카ード110固有の公開暗号鍵Kpmlおよびメモ리카ード110における禁止クラスリストのバージョンデータCRL\_verを受信する(ステップS126)。

【0103】禁止クラスリストのバージョン情報CRL\_verは、データバスBS1を介して配信制御部315に送られ、配信制御部315は、受理したバージョンデータCRL\_verに従って、当該CRL\_verのバージョンとCRLデータベース306内の禁止クラスリストデータの現在のバージョンとの間の変化を表わす差分データCRL\_datを生成する(ステップS128)。

【0104】さらに、配信制御部315は、ステップS106で取得したコンテンツIDおよびライセンス購入条件データACに従って、ライセンスID、アクセス制限情報AC1および再生回路制御情報AC2を生成する(ステップS130)。さらに、暗号化コンテンツデータを復号するためのライセンスキーKcを情報データベース304より取得する(ステップS132)。

【0105】図9を参照して、配信制御部315は、生成したライセンス、すなわち、ライセンスキーKc、再生回路制御情報AC2、ライセンスID、コンテンツID、およびアクセス制限情報AC1を暗号化処理部326に与える。暗号化処理部326は、復号処理部320によって得られたメモ리카ード110固有の公開暗号鍵Kpmlによってライセンスを暗号化する(ステップS136)。暗号化処理部328は、暗号化処理部326の出力と、配信制御部315がデータバスBS1を介して供給する禁止クラスリストの差分データCRL\_datとを受けて、メモ리카ード110において生成されたセッションキーKs2によって暗号化する。暗号化処理部328より出力された暗号化データは、データバスBS1および通信装置350を介して携帯電話機100に送信される(ステップS138)。

【0106】このように、配信サーバおよびメモ리카ードでそれぞれ生成される暗号鍵をやり取りし、お互いが受領した暗号鍵を用いた暗号化を実行して、その暗号化データを相手方に送信することによって、それぞれの暗

号化データの送受信においても事実上の相互認証を行なうことができる。

【0107】携帯電話機100は、送信された暗号化データ {Kc//AC2//ライセンスID//コンテンツID//AC1} Km1//CRL\_dat} Ks2を受信し(ステップS140)、メモリインタフェース1200を介してメモ리카ード110へ出力する。メモ리카ード110においては、メモリインタフェース1200を介して、データベース3に与えられた受信データを復号処理部1412によって復号する。復号処理部1412は、セッションキー発生部1418から与えられたセッションキーKs2を用いてデータベース3の受信データを復号しデータベース4に出力する(ステップS142)。

【0108】この段階で、データベース4には、Km1保持部1421に保持される秘密復号鍵Km1で復号可能な暗号化ライセンス {Kc//AC2//ライセンスID//コンテンツID//AC1} Km1と、CRL\_datとが出力される。コントローラ1420の指示によって、暗号化ライセンス {Kc//AC2//ライセンスID//コンテンツID//AC1} Km1は、メモリ1415に記録される(ステップS144)。一方、暗号化ライセンス {Kc//AC2//ライセンスID//コンテンツID//AC1} Km1は、復号処理部1422において、秘密復号鍵Km1によって復号され、ライセンスのうち、メモ리카ード110内で参照されるライセンスID、コンテンツIDおよびアクセス制限情報AC1のみが受理される(ステップS146)。

【0109】コントローラ1420は、受理したCRL\_datに基づいて、メモリ1415内の禁止クラスリストデータCRLおよびそのバージョンを更新する(ステップS148)。さらに、ライセンスID、コンテンツIDおよびアクセス制限情報AC1については、ライセンス情報保持部1440に記録される(ステップS150)。

【0110】ステップS150までの処理がメモリ回路で正常に終了した段階で、携帯電話機100から配信サーバ30にコンテンツデータの配信要求がなされる(ステップS152)。

【0111】配信サーバ30は、コンテンツデータの配信要求を受けて、情報データベース304より、暗号化コンテンツデータ {Data} Kcおよび付加情報Data-infを取得して、これらのデータをデータベース1および通信装置350を介して出力する(ステップS154)。

【0112】携帯電話機100は、{Data} Kc//Data-infを受信して、暗号化コンテンツデータ {Data} Kcおよび付加情報Data-infを

受理する(ステップS156)。暗号化コンテンツデータ {Data} Kcおよび付加情報Data-infは、メモリインタフェース1200および端子1201を介してメモ리카ード110のデータベース3に伝達される。メモ리카ード110においては、受信した暗号化コンテンツデータ {Data} Kcおよび付加情報Data-infがそのままメモリ1415に記録される(ステップS158)。

【0113】さらに、メモ리카ード110から配信サーバ30へは、配信受理の通知が送信され(ステップS160)、配信サーバ30で配信受理を受信すると(ステップS162)、課金データベース302への課金データの格納等を行って、配信終了の処理が実行され(ステップS164)、全体の処理が終了する(ステップS170)。

【0114】このようにして、携帯電話機100に装着されたメモ리카ード110が正規の機器であること、同時に、クラス証明書Cmc1とともに暗号化して送信できた公開暗号鍵Kp1およびKpmc1が有効であることを確認した上で、それぞれのクラス証明書Cmc1が禁止クラスリスト、すなわち、公開暗号鍵Kp1およびKpmc1による暗号化が破られたクラス証明書リストに記載されていないメモ리카ードからの配信要求に対してのみコンテンツデータを配信することができ、不正なメモ리카ードへの配信および解読されたクラス鍵を用いた配信を禁止することができる。

【0115】次に、メモ리카ード110に配信されたコンテンツデータの携帯電話機100における音楽再生に関する処理について、図10を用いて説明する。

【0116】メモ리카ード110は、メディア内にある曲データおよびライセンス情報をメモリ1415に記録している。携帯電話機100は、メモ리카ード内110の曲情報を取り出し、メディア内曲リストR1として生成し、メモリ1230に記録する。

【0117】メディア内曲リストR1は、暗号化コンテンツデータ {Data} Kcとともに配信サーバ30から送信されるメタデータから曲名等の主要な関連情報を抽出して作成されたものである。

【0118】メディア内曲リストR1は、図10(a)に示すように、記録される各曲データの特性を示す特性リスト500と、記録される各曲データの曲名とアーティスト名とを示す曲名・アーティスト名リスト501とから成る。

【0119】図において、特性リスト500には、再生番号001~006、“L”、“C”が記録され、曲名・アーティスト名リスト501には、曲名1~11と対応するアーティスト名A~Fとが記録されている。

【0120】特性リスト500の再生番号は、再生可能な曲データに割当てられた番号である。

【0121】特性リスト500に、“L”が記録されて

いる曲は、メモリカード110に暗号化コンテンツデータ{Data}Kcだけが存在しライセンスキーKcがないことを示す。たとえば、携帯電話機のユーザ1が、パソコンや他の携帯電話機のユーザ2等から暗号化コンテンツデータ{Data}Kcをコピーしたり、ダウンロードした場合がこれに相当する。

【0122】特性リスト500に、“C”が記録されている曲は、メモリカード110にライセンスキーKcは存在するが暗号化コンテンツデータ{Data}Kcが存在しないことを示す。たとえば、ユーザ1がメモリカード110内にライセンスキーと暗号化コンテンツデータとを持っていた状態で、パソコン等などを用いて他の記録媒体に暗号化コンテンツデータ{Data}Kcを移動することで、メモリカード110から暗号化コンテンツデータ{Data}Kcが削除された場合がこれに相当する。また、携帯電話機のユーザ2が、携帯電話機のユーザ1から暗号化コンテンツデータ{Data}Kcを受け、ユーザ1の携帯電話機から当該暗号化コンテンツデータ{Data}Kcが削除された場合もこれに相当する。

【0123】携帯電話機100は、コントローラ1106の制御に基づき、再生モード時に再生曲リストR2を生成する。再生曲リストR2は、メモリ1230に記録される。再生曲リストR2は、図10(b)に示すように、再生番号を示す再生番号リスト510と、曲名・アーティスト名リスト511とから成る。

【0124】再生曲リストR2は、メディア内曲リストR1に記録される曲データのうちコンテンツデータとライセンスデータとが揃った再生可能な曲データを抽出して作成される。より具体的には、再生曲リストR2は、再生番号を有する曲データに基づき生成される。

【0125】再生曲リストR2は、たとえば、携帯電話機100のディスプレイ1110に表示される。ユーザは、表示される再生曲リストR2のなかから再生する曲を選択する。

【0126】第1の実施の形態では、ライセンスによる制限に基づき、メディア内曲リストR1が更新される。そして、メディア内曲リストR1に従って再生曲リストR2が更新される。

【0127】たとえば、図11(a)に示す再生番号004の曲名8/アーティストDについて、ライセンスが再生期日の制限がついていた場合、ライセンスで指定される再生期日が過ぎた時には、図11(b)に示すように再生番号004が特性“LN”に変わる。また、ライセンスで制限されるのが再生回数であった場合、ライセンスにより再生回数が制限値に到達した時にも、再生番号が、ライセンス制限により再生できないことを示す記号(たとえば、“LC”)に変わる。

【0128】たとえば、図12(a)に示すように、再生曲リストR2のうち再生番号001~006が付され

る曲名1, 3, 4, 8, 10, 11から選曲を行うとする。再生番号004に再生回数制限があるとする。再生番号004が、再生回数分だけ再生された場合、図12(b)に示すように再生番号004が再生曲リストから削除される。そして、図12(c)に示すように再生番号が自動的に修正され、曲名1, 3, 8, 11に対して再生番号001, 002, 003, 004, 005が割当てられる。

【0129】次に、携帯電話機100におけるコンテンツデータの再生動作の流れについて説明する。

【0130】図13を参照して、初期状態として待ち受け状態にあるとする。音楽再生モードに入ると(ステップS200)、コントローラ1106は、データバスBS2を介して認証データ保持部1202から認証データ{Kp1//Crtf1}Kpmaを読み出し、メモリーインタフェース1200を介してメモリカード110へ認証データ{Kp1//Crtf1}Kpmaを入力する(ステップS201)。

【0131】メモリカード110は、認証データ{Kp1//Crtf1}Kpmaを受理する(ステップS202)。そして、メモリカード110の復号処理部1408は、受理した認証データ{Kp1//Crtf1}Kpmaを、Kpma保持部1414に保持された公開認証鍵Kpmaによって復号し(ステップS203)、コントローラ1420は復号処理部1408における復号処理結果から、認証処理を行なう。すなわち、認証データ{Kp1//Crtf1}Kpmaが正規の認証データであるか否かを判断する認証処理を行なう(ステップS204)。

【0132】認証データが復号できなかった場合、コントローラ1420は認証データ不受理の出力をデータバスBS3および端子1201を介して携帯電話機100のメモリーインタフェース1200へ出力する(ステップS230)。そして再生不能の表示を行ない(ステップS231)、音楽再生モードを終了する。

【0133】認証データが復号できた場合、コントローラ1420は、取得した証明書Crtf1がメモリー1415から読出した禁止クラスリストデータに含まれるか否かを判断する(ステップS205)。この場合、証明書Crtf1にはIDが付与されており、コントローラ1420は、受理した証明書Crtf1のIDが禁止クラスリストデータの中に存在するか否かを判別する。証明書Crtf1が禁止クラスリストデータに含まれると判断されると、コントローラ1420は認証データ不受理の出力をデータバスBS3および端子1201を介して携帯電話機100のメモリーインタフェース1200へ出力する(ステップS230)。

【0134】ステップS204において認証データが公開認証鍵Kpmaで復号できなかったと、およびステップS205において受理した証明書Crtf1が禁止

クラスリストデータに含まれているとき、認証データ不受理の出力がなされる。そして、携帯電話機100のコントローラ1106は、認証データ不受理のため再生不可であることをディスプレイ1110に表示する。

【0135】ステップS205において、証明書Cnf1が禁止クラスリストデータに含まれていないと判断されると、再生曲リストR2が生成され、表示される（ステップS206）。再生曲リストR2が表示されると、ユーザによる選曲モードになる（ステップS207）。

【0136】選曲されると、図14を参照して、メモリカード110のセッションキー発生部1418は、再生セッション用のセッションキーKs2を発生させる（ステップS208）。そして、暗号化処理部1410は、セッションキー発生部1418からのセッションキーKs2を、復号処理部1408で復号された公開暗号鍵Kp1によって暗号化した{Ks2}Kp1をデータベースBS3へ出力する（ステップS209）。そうすると、コントローラ1420は、端子1201を介してメモリインタフェース1200へ{Ks2}Kp1を出力し、携帯電話機100のコントローラ1106は、メモリインタフェース1200を介して{Ks2}Kp1を取得する。そして、Kp1保持部1204は、秘密復号鍵Kp1を復号処理部1206へ出力する。

【0137】復号処理部1206は、Kp1保持部1204から出力された、公開暗号鍵Kp1と対になっている秘密復号鍵Kp1によって{Ks2}Kp1を復号し、セッションキーKs2を暗号化処理部1208へ出力する（ステップS210）。そうすると、セッションキー発生部1210は、再生セッション用のセッションキーKs3を発生させ、セッションキーKs3を暗号化処理部1208へ出力する（ステップS211）。暗号化処理部1208は、セッションキー発生部1210からのセッションキーKs3を復号処理部1206からのセッションキーKs2によって暗号化して{Ks3}Ks2を出力し、コントローラ1106は、データベースBS2およびメモリインタフェース1200を介して{Ks3}Ks2をメモリカード110へ出力する（ステップS212）。

【0138】メモリカード110の復号処理部1412は、端子1201およびデータベースBS3を介して{Ks3}Ks2を入力し、セッションキー発生部1418によって発生されたセッションキーKs2によって{Ks3}Ks2を復号して、携帯電話機100で発生されたセッションキーKs3を取得する（ステップS213）。

【0139】セッションキーKs3の受理に応じて、コントローラ1420は、ライセンス情報保持部1440内の対応するアクセス制限情報AC1を確認する（ステップS214）。

【0140】ステップS214においては、メモリのアクセスに対する制限に関する情報であるアクセス制限情報AC1を確認する。再生不可の状態である場合には再生動作を終了し、再生回数に制限がある場合にはアクセス制限情報AC1のデータを更新し再生可能回数を更新する。そして、次のステップに進む（ステップS215）。アクセス制限情報AC1が更新されると、携帯電話機100側においてもメディア内曲リストR1も更新される。

【0141】アクセス制限情報AC1によって再生回数が制限されていない場合においては、ステップS215はスキップされ、アクセス制限情報AC1は更新されることなく次の処理に進む（ステップS216）。

【0142】ステップS214において、当該再生動作において再生が可能であると判断された場合には、選曲された曲データのライセンスキーKcを含むライセンスの復号処理が実行される。具体的には、コントローラ1420の指示に応じて、メモリ1415からデータベースBS4に読出された暗号化ライセンス{Kc//AC2//ライセンスID//コンテンツID//AC1}Kmlを復号処理部1422がメモリカード110固有の秘密復号鍵Kmlによって復号し、再生処理に必要なライセンスキーKcと再生回路制御情報AC2がデータベースBS4上に得られる（ステップS216）。

【0143】得られたライセンスキーKcと再生回路制御情報AC2は、切換スイッチ1444の接点Pdを介して暗号化処理部1406に送られる。暗号化処理部1406は、切換スイッチ1444の接点Pdを介して復号処理部1412より受けたセッションキーKs3によってデータベースBS4から受けたライセンスキーKcと再生回路制御情報AC2とを暗号化し、{Kc//AC2}Ks3をデータベースBS3に出力する（ステップS217）。

【0144】データベースBS3に出力された暗号化データは、メモリインタフェース1200を介して携帯電話機100に送出される。

【0145】携帯電話機100においては、メモリインタフェース1200を介してデータベースBS2に伝達される暗号化データ{Kc//AC2}Ks3を復号処理部1212によって復号処理を行い、ライセンスキーKcおよび再生回路制御情報AC2を受理する（ステップS218）。復号処理部1212は、ライセンスキーKcを復号処理部1214に伝達し、再生回路制御情報AC2をデータベースBS2に出力する。

【0146】コントローラ1106は、データベースBS2を介して、再生回路制御情報AC2を受理して再生の可否の確認を行なう（ステップS219）。

【0147】ステップS219においては、再生回路制御情報AC2によって再生不可と判断される場合には、再生動作は終了される。

【0148】ステップS219において再生可能と判断された場合、コントローラ1106は、メモリインタフェース1200を介してメモリカード110に暗号化コンテンツデータ{Data}Kcを要求する。そうすると、メモリカード110のコントローラ1420は、メモリ1415から暗号化コンテンツデータ{Data}Kcを取得し、データバスBS3および端子1201を介してメモリインタフェース1200へ出力する(ステップS220)。

【0149】携帯電話機100のコントローラ1106は、メモリインタフェース1200を介して暗号化コンテンツデータ{Data}Kcを取得し、データバスBS2を介して暗号化コンテンツデータ{Data}Kcを復号処理部1214へ与える。そして、復号処理部1214は、暗号化コンテンツデータ{Data}Kcを復号処理部1212から出力されたコンテンツ鍵Kcによって復号してコンテンツデータDataを取得する(ステップS221)。

【0150】そして、復号されたコンテンツデータDataは音楽再生部1216へ出力され、音楽再生部1216は、コンテンツデータを再生し、DA変換器1218はデジタル信号をアナログ信号に変換して端子1220へ出力する。そして、スイッチ1222は端子1220を選択して音楽データは端子1224を介してヘッドホン130へ出力されて再生される(ステップS222)。

【0151】そして、選曲されたコンテンツデータの再生動作が終了すると、更新されたメディア内曲リストR1に基づき再生曲リストR2が生成され、再表示される(S223)。

【0152】選曲(ステップS207)により複数の曲が、または同一曲が複数回選択された時には、表示動作(ステップS223)が終了する毎に、たとえば、図14のステップS208の処理に移る。

【0153】このように、第1の実施の形態によれば、携帯電話機は、コンテンツデータの著作権を十分に保護しながら再生することができる。特に、ライセンスの制限を自動的に判別できるため、ユーザー側の選曲動作が簡単化される。

【0154】メディア内曲リストR1は、メモリカード110側へ転送し、メモリカード110側のメモリ1415にも格納する。

【0155】なお、第1の実施の形態では、再生曲リストR2は、再生可能な曲データに関する情報を含むようにしたが、これに限定されない。メディア内曲リストR1と同様に、暗号化コンテンツデータとライセンスキーが存在する、暗号化コンテンツデータのみが存在しライセンスキーが存在しない、ライセンスキーが存在するが暗号化コンテンツデータが存在しない、その他ライセンスによる制限に関する情報を含ませ、これらの特性を

表示するようにしてもよい。

【0156】この場合、再生不可能な曲データが選曲されると、コントローラ1106は、再生処理を実行せず、に、再生に必要なデータをダウンロードするか、当該曲データを削除するかをユーザに促すメッセージをディスプレイ1110に表示する。そして、ユーザの選択に従って、ダウンロード処理や削除を実行するようにする。これにより、ユーザによる記録データの管理が簡単化される。

【0157】[第2の実施の形態]第1の実施の形態では、メディア内曲リストR1を携帯電話機100で生成(更新)した。これに対し、第2の実施の形態では、メモリカード110においてメディア内曲リストR1を生成する。

【0158】この場合、メモリカード110におけるコントローラ1420が、メモリカード110に格納されるデータに基づき、メディア内曲リストR1を生成する。メディア内曲リストR1は、携帯電話機100のコントローラ1106の要求に応じて携帯電話機100側に転送される。

【0159】そして、コントローラ1106は、再生モード時に、当該メディア内曲リストR1に基づき再生曲リストR2を生成し、表示する。

【0160】この場合であっても、第1の実施の形態と同様に、携帯電話機は、コンテンツデータの著作権を十分に保護しながら再生することができる。また、ライセンスの制限を自動的に判別できるため、ユーザー側の選曲動作が簡単化される。

【0161】[第3の実施の形態]第3の実施の形態による携帯電話機100およびメモリカード110について説明する。携帯電話機100およびメモリカード110の構成は、第1の実施の形態で説明したとおりである。

【0162】第3の実施の形態による携帯電話機100は、メディア内曲リストを管理するメディア管理モードを有する。メディア内曲リストを管理するメディア管理モードについて、図15を用いて説明する。

【0163】メディア内曲リストR1に携帯電話機100からアクセスする前に、メモリカード110と携帯電話機100との間の認証がすでになされているものとする。

【0164】まず、待ち受け状態にあるとする(ステップS300)。ユーザによるモード指定がなされると、メディア管理モードであるか否かが判断される(ステップS302)。メディア管理モードでない場合(たとえば、上述した音楽再生モード等)は、該当する処理モードを実行する(ステップS310)。

【0165】メディア管理モードである場合、携帯電話機100は、メモリカード110側からデータを手する(ステップS304)。

【0166】そして、携帯電話機100は、当該データに基づき、メディア内曲リストR1をディスプレイ110に表示する(ステップS306)。表示では、特性リスト500にある特性“C”(コンテンツデータがない)、“L”(ライセンスキーがない)、“LC”(ライセンスによる制限があり、制限を越えた)、コンテンツデータとライセンスキーとが存在する等をユーザーが認識できるように表示する。なお、色による区別をつけてもよい。

【0167】表示内容は、これに限定されず、特性“C”(ライセンスのみの曲)、“L”(コンテンツのみの曲)、“LC”(再生の回数制限を越えた曲)、“LN”(再生の時間制限を越えた曲)の他にライセンス制限がある曲の表示マークがあってもよい。

【0168】そして、メディア内曲リストR1のデータ編集を行う(ステップS308)。編集処理において、ライセンスまたは/およびコンテンツデータの削除、再生番号の順番の変更が可能となる。編集の途中経過、および結果は、すべてディスプレイ110に表示される。

【0169】なお、各曲データに個人的な情報付加することも可能である。ただし、ライセンスキーやコンテンツデータの改ざんはできない。

【0170】編集後、メディア内曲リストR1をメモ리카ード110に転送する。このように、第3の実施の形態によれば、コンテンツに関連するデータをユーザー側で編集することができるため、ユーザー側の意向にそったデータ管理が可能になる。

【0171】[第4の実施の形態] 第3の実施の形態では、メディア内曲リストR1を携帯電話機100で生成し、編集する場合について説明した。これに対し、第4の実施の形態では、メモ리카ード110でメディア内曲リストR1を生成し、携帯電話機100で編集する場合について説明する。

【0172】この場合、携帯電話機100は、メディア管理モードになると、図15に示すステップS304の代わりに、メモ리카ード110からメディア内曲リストR1を読出す処理を行う。そして、メモ리카ード110から受取ったメディア内曲リストR1をステップS306で表示する。

【0173】そして、ステップS308において、メディア内曲リストR1のデータ編集を行う。編集処理においては、たとえば、再生番号の順番の変更が可能となる。編集の途中経過、および結果は、すべてディスプレイ110に表示される。

【0174】編集後、メディア内曲リストR1をメモ리카ード110に転送する。このように、第4の実施の形態によれば、コンテンツに関連するデータをユーザー側で編集することができるため、ユーザー側の意向にそったデータ管理が可能になる。

【0175】[第5の実施の形態] 第1の実施の形態では、メディア内曲リストR1の更新に基づき、再生曲リストR2を更新した。これに対し、第5の実施の形態では、音楽再生モード中は、再生曲リストR2を直接ライセンスの制限に従って更新する。

【0176】このため、第5の実施の形態では、音楽再生モードが開始されると、携帯電話機は、携帯電話機内においてアクセスに関する情報を管理する。たとえば、第1の実施の形態による構成では、携帯電話機100側にアクセスに関する情報(アクセス制限情報ACK1)を転送する。転送後、携帯電話機は、携帯電話機100内においてアクセスに関する情報を管理する。携帯電話機で管理するアクセスに関する情報を、再生回数に関する情報ACK1と称す。

【0177】なお、暗号・復号方式、認証方式は第1の実施の形態によるものには限定されない。再生側として携帯電話機(たとえば、携帯電話機100)を、メディア側としてメモ리카ード(たとえば、メモ리카ード110)を代表例として説明する。以下の説明では、メモ리카ード側における携帯電話機に対する認証は正当であるものとする。

【0178】第5の実施の形態による音楽再生モードでの処理の概要について、図16を用いて説明する。まず、待ち受け状態にある(ステップS400)。指示に従いモード判定を行う(ステップS402)。なお、音楽再生モードであると判定されると、メディア内曲リストR1に基づき、再生曲リストR2が生成され、ディスプレイ110に表示される(ステップS404)。

【0179】音楽再生要求(選曲)があるか否かが判定される(ステップS406)。再生要求がない場合には、ステップS404に移る。

【0180】音楽再生要求があると、選曲された曲データが、ライセンスにより再生回数に制限があるか否かが判定される(ステップS408)。制限がなければ、暗号化コンテンツデータを所定の形式で復号して、音楽を再生する(ステップS422)。そして、音楽終了要求があるか否かが判定され(ステップS424)、終了要求があればステップS404へ、終了要求が無ければステップS422の再生状態を継続する。

【0181】ライセンスにより再生回数に制限のある曲を再生する場合には、再生回数が限度に達したか否かが判断される(ステップS410)。再生回数が最終でない場合には、再生回数に関する情報ACK1を更新する(ステップS420)。そして、ステップS422の処理に移る。

【0182】再生回数が最後の再生であった場合には、音楽を再生する処理(ステップS412)に移る。そして、音楽終了要求があるか否かが判定され(ステップS414)、終了要求があればステップS416へ、終了要求が無ければステップS412の再生状態を継続す

る。

【0183】再生回数が最後の再生後に音楽終了要求があると、再生曲リストR2から再生した曲データを削除し、再生曲リストR2を再構築する(ステップS416)。これにより、再生可能な曲データのリストと、対応する再生番号が修正される。

【0184】そして、曲を再生する度にメディア内曲リストR1を更新し、対応する曲データについて、ライセンスにより再生できない旨を示すマーク(たとえば、“LC”)をつける(ステップS418)。

【0185】音楽再生モードが終了すると、メディア内曲リストR1は、メモ리카ード110に転送される。

【0186】このように、第5の実施の形態では、音楽再生モードに入ると、携帯端末側(再生系側)で、ライセンスによる制限に基づき再生曲リストR2が自動的に更新される。

【0187】これにより、第1の実施の形態と同様、ライセンスの制限を自動的に判別できるため、ユーザ側の選曲動作が簡便化される。

【0188】なお、上記説明では再生回数だけに限定して説明したが、ライセンスにより制限のあるものであればいずれにも適用される。

【0189】今回開示された実施の形態はすべての点で例示であって制限的なものではないと考えられるべきである。本発明の範囲は、上記した実施の形態の説明ではなくて特許請求の範囲によって示され、特許請求の範囲と均等の意味および範囲内でのすべての変更が含まれることが意図される。

【図面の簡単な説明】

【図1】 データ配信システムを概念的に説明する概略図である。

【図2】 図1に示すデータ配信システムにおける通信のためのデータ、情報等の特性を示す図である。

【図3】 図1に示すデータ配信システムにおける通信のためのデータ、情報等の特性を示す図である。

【図4】 図1に示すデータ配信システムにおける通信のためのデータ、情報等の特性を示す図である。

【図5】 ライセンスサーバの構成を示す概略ブロック図である。

【図6】 携帯電話機の構成を示すブロック図である。

【図7】 メモ리카ードの構成を示すブロック図である。

【図8】 図1に示すデータ配信システムにおける配信

動作を説明するための第1のフローチャートである。

【図9】 図1に示すデータ配信システムにおける配信動作を説明するための第2のフローチャートである。

【図10】 (a) メディア内曲リストR1、(b) 再生曲リストR2をそれぞれ示す概念図である。

【図11】 (a)、(b)は、メディア内曲リストR1の更新状況を説明するための概念図である。

【図12】 (a)、(b)、(c)は、再生曲リストR2の更新状況を説明するための概念図である。

【図13】 携帯電話機における再生動作を説明するための第1のフローチャートである。

【図14】 携帯電話機における再生動作を説明するための第2のフローチャートである。

【図15】 携帯電話機におけるメディア管理モードでの処理内容を説明するためのフローチャートである。

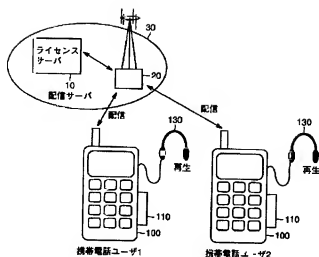
【図16】 第5の実施の形態による音楽再生モードでの処理動作を説明するためのフローチャートである。

【符号の説明】

10 ライセンスサーバ、20 配信キャリア、30 配信サーバ、100 携帯電話機、110 メモ리카ード、130 ヘッドホン、140 コンピュータ、141 ハードディスク、142、1106、1420 コントローラ、143 外部インタフェース、144 ライセンス保護モジュール、145 通信ケーブル、302 課金データベース、304 情報データベース、306 CRLデータベース、310 データ処理部、312、320、1206、1212、1214、1404、1408、1412、1422 復号処理部、315 配信制御部、316、1210、1418 セッションキー発生部、318、326、328、1208、1410 暗号化処理部、350 通信装置、1102 アンテナ、1104 送受信部、1108、1224 キー操作部、1110 ディスプレイ、1112 音声再生部、1113、1218 DA変換器、1114、1201、1220、1224 端子、1200 メモリインタフェース、1222 スイッチ、1402 Kmc1保持部、1414、1414B Kpma保持部、1415 メモリ、1416 Kpm1保持部、1421 Km1保持部、1440 ライセンス情報保持部、1442、1444、1446 切換スイッチ、1202、1400 認証データ保持部、1204 Kp1保持部、1216 音楽再生部。



【図1】



【図2】

名称	属性	保持/発生箇所	機能・特徴
Data	コンテンツデータ	配信サーバ	例：音楽データ
Kc	ライセンスキー		暗号化コンテンツデータの復号鍵
[Data]Kc	暗号化コンテンツデータ		本装置Kcで復号可能な暗号化されたコンテンツデータ この形式で配信サーバより配布
Data-inf	付加情報		例：コンテンツデータに関する著作権あるいはサーバアクセス関連等の平文情報
コンテンツID	コンテンツに関する情報		コンテンツデータDataを識別するコード
ライセンスID	ライセンスに関する情報		ライセンスの発行を特定できる管理コード (コンテンツIDを含めて識別することも可)
AC	ライセンス購入条件		利用条件から推定(例：ライセンス版、機能限定等)
AC1	アクセス制限情報		メモリのアクセスに対する制限(例：再生可能回数)
AC2	再生回数の制限情報		コンテンツ再生回数(携帯電話機)における制限情報 (例：再生回可)

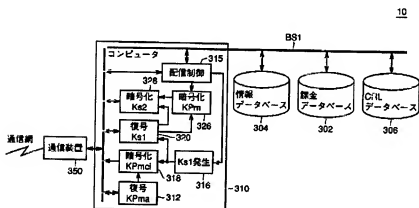
【図3】

名称	属性	保持/発生箇所	機能・特徴
CRL	停止クラスリスト	配信サーバ メモ리카ード	停止クラスリストの対象クラスデータ
CRL_dat	停止クラスリスト関連情報	配信サーバ	停止クラスリストのバージョン更新のための情報 (差分データ形式)
CRL_ver		メモ리카ード	停止クラスリストのバージョン情報
KPpn	公開暗号鍵 (非対称鍵)	携帯電話機	Kpncにて復号可能。 (KPpn/Crtn/KPmaの形式で出荷時に記録 ※携帯電話機の電源nごとに異なる)
KPmcl	公開暗号鍵 (非対称鍵)	メモ리카ード	Kmclにて復号可能。 (KPmcl/Cmcl/KPmaの形式で出荷時に記録 ※メモ리카ードの種類ごとに異なる)
Kpni	秘密復号鍵	携帯電話機	コンテンツ再生回路(携帯電話機)固有の復号鍵 ※携帯電話機の電源nごとに異なる
Kmci	秘密復号鍵	メモ리카ード	メモ리카ード固有の復号鍵 ※メモ리카ードの種類ごとに異なる
Crtn	クラス証明書	携帯電話機	コンテンツ再生回路のクラス証明書。認証機能を有する。 (KPpn/Crtn/KPmaの形式で出荷時に記録 ※携帯電話機の電源nごとに異なる)
Cmci		メモ리카ード	メモ리카ードのクラス証明書。認証機能を有する。 (KPmcl/Cmcl/KPmaの形式で出荷時に記録 ※メモ리카ードの電源nごとに異なる)

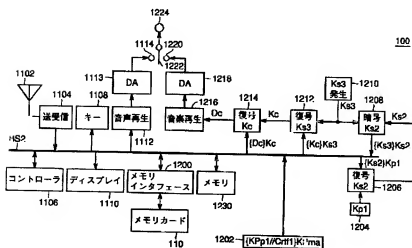
【图4】

名称	属性	保持/発生箇所	機能・特徴
Ks1	共通部	記憶サーバ	記憶セッション部に発生
Ks2		メモリカード	記憶/再生セッション部に発生
Ks3		携帯電話機	再生セッション部に発生
Km		秘密復号鍵	メモリカードごとに固有の復号鍵
KPm	公開暗号鍵 (非対称鍵)	メモリカード	KPmで暗号化されたデータはKmで復号可能
KPma	公開証証鍵	記憶サーバ	応用システムを特で共通。

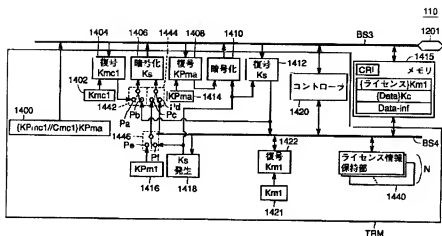
【图5】



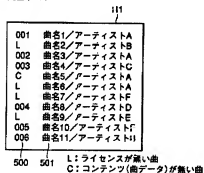
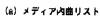
【図6】



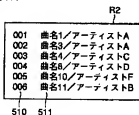
【例7】



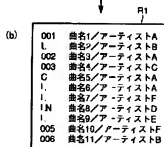
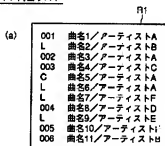
【图 10】



(b) 再生産リスト



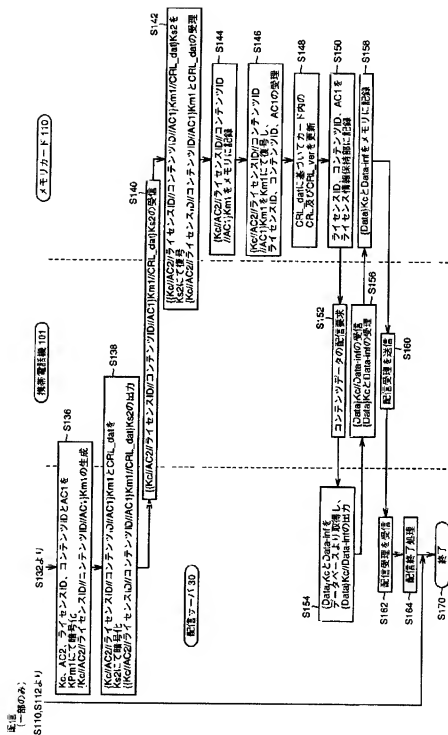
【例 11】



LN: ライセンスは存在するが期限が切れた由

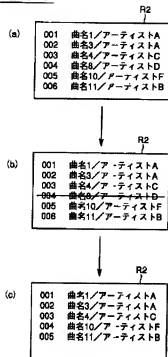


【図9】

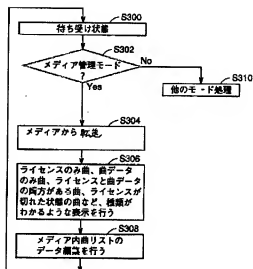


【図12】

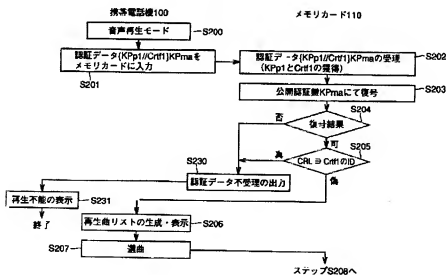
再生曲リスト



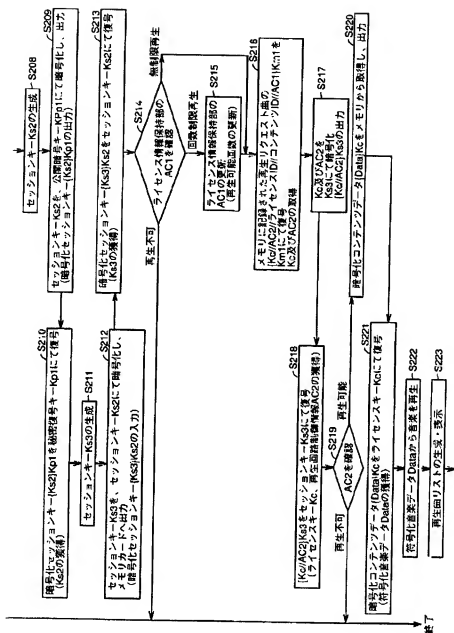
【図15】



【図13】



【図14】



【図16】

